Foreword

The various defenses Shikari Inc. Should take in opposition to Ludens Inc.'s allegations resulting from the data breach that occurred on the "***Data Breach***" are covered in this note. This remark is based on the facts and assumptions listed below:

A: A certain amount of Ludens' data was taken because of the Data Breach. Data set contains:

- Client information, such as customer lists, papers showing Ludens' marketing plan, sales, turnover, and financial information

- Papers outlining the technology behind Ludens' equipment and identifying the patents that protect their diagnostic tools (projects and drawings, manufacturing and maintenance manuals, user manuals)

- Personal information pertaining to certain individuals that were identified utilizing Ludens' diagnostic equipment ("***Health Data***")

B: In response to the data breach, Ludens sent Shikari a letter of caution requesting payment for the purported losses brought on by the data breach. Ludens makes the following claims:

- Shikari broke its duty of confidentiality, causing information to become public and Ludens to lose its competitive edge. Ludens' Know-How was proprietary information that gave Ludens an advantage over its rivals (***the "Breach of Confidence Claim***").

• The patients whose diagnoses and treatments used Ludens' tools are the subject of the health data. Shikari is responsible for the GDPR violation of failing to stop the processing of Health Data by an unauthorized third party (the ***"Data Protection Claim***").

Executive Summary

Our preliminary study suggests the following, subject to the actions and analyses described in this note:

A: Shikari might counter the Breach of Confidentiality Claim with the following arguments:

• Because Ludens' know-how has been revealed or is in the public domain (for example, because it is the topic of patent filings that are accessible in the databases of the patent offices), it could not be considered a trade secret. In any case.

• Because Shikari never agreed to this responsibility in writing or because Shikari took all reasonable precautions to store the Data, Shikari may not be accountable to Ludens for a breach of confidentiality. As a result, the Data Breach cannot be attributed to Shikari's negligence.

B: To refute the Data Protection Claim, Shikari may make the following claims:

• If Health Data are anonymized and aggregated, they won't likely meet the GDPR's definition of "personal data," ensuring that no unauthorized processing of personal data took place because of the data breach; and, in any case,

• If Health Data is personal information, Ludens would be the data controller responsible for making sure they are safeguarded in a way that prevents unauthorized processing by third parties. If

Shikari is the data processor; it must have followed Ludens' instructions forLudens to be held accountable for failing to identify sufficient security measures.

C: In any case, it is the affected party's responsibility to prove their losses and the cause of them (i.e., Ludens).

Shikari might employ a defensive strategy

Ludens' Breach of Confidence Claim

A: Summarizing Ludens' assertion: We comprehend that the following factual and legal justifications underpin Ludens' Breach of Confidentiality Claim:

- Because it is a trade secret, Ludens' know-how has economic worth if it is kept a secret.
- The service agreement between Shikari, as the colocation service provider, and Ludens, as the customer, requires Shikari to comply with two obligations:

  (1) preventing unauthorized third parties from accessing Ludens' Data; and

  (2) maintaining confidentiality, and
- Shikari's infringement of its contractual obligations led to the Data Breach.

B: Shikari's possible counterarguments According to our preliminary analysis, Shikari may employ the following defenses to fight the Breach of Confidentiality Claim, subject to the activities listed in paragraph (c) below:

- It's possible that Ludens' Know-How is not a trade secret:

  (a) It is the responsibility of Ludens to demonstrate that the Know-How was secret, and that Ludens took reasonable security precautions to protect its confidentiality.

  (b) Technical know-how that was disclosed in patent filings does not count as a trade secret. The competent patent office’s publish patent files (after an initial non-disclosure period).

(c) Like how client financial and accounting information that is released publicly (such as in the financial statements of the firm) does not qualify as a trade secret.

- If contractual assessment reveals that Shikari had no obligation to safeguard Ludens' Know-How from unauthorized access or to keep it confidential, it may be assumed that Ludens' Know-How is a trade secret. The colocation service agreement, for instance, may just provide that Shikari's responsibility is to store data on behalf of Ludens, with no mention of Shikari assuming responsibility for any loss or theft,

- If Shikari could prove that it met its duties with the necessary diligence and that no Shikari error was responsible for the Data Breach, then, assuming Shikari had a duty to protect data from loss or theft, Shikari would not be liable to Ludens. Shikari's credentials might improve his or her standing, and

- For example, if Ludens' Commercial Know-How does not have economic value (for example, because it is "basic" know-how for someone operating in the same business), Ludens may not claim damages; or, if Ludens' files were encrypted using advance encryption technologies, it should not be assumed that these files are readable or that Ludens suffered damages as a result of the Data Breach.

C: Future steps: The following steps should be taken to strengthen Shikari's defense plan:

- Shikari will investigate the data breach, determine what caused it, and determine any mistakes the Shikari team could have made,

- To evaluate the contractual framework of Shikari's responsibilities and liabilities vis-à-vis Ludens, our firm will analyze the colocation services agreement and any additional agreements between Shikari and Ludens,

- If Shikari is aware of the Data kept by Ludens on its servers, Shikari must give a report outlining the kind of Data, the types of files, and the security precautions used by Ludens (e.g., passwords, encryption, etc.), and

- To find out if certain Data were already in the public domain prior to the data breach, our company searched publicly accessible databases (such IP databases).

Ludens' Data Protection Claim

A: We recognize that Ludens' Data Protection Claim is supported by the following factual and legal justifications:

- According to the definition of "personal data" in **Article 4 of the GDPR**, the health data Shikari keeps on behalf of Ludens falls under its jurisdiction, and

- According to **GDPR Article 5(1)(f)**, Shikari is responsible for not taking "appropriate ***technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction***."

B: Shikari's possible counterarguments: Our preliminary research showed that Shikari may employ the following defenses to counter the Data Protection Claim, subject to the steps mentioned in paragraph (c) below:

- Based on what we understand, Ludens aggregates and anonymizes health data before selling the dataset of anonymous data to hospitals and researchers. Shikari may contend that the GDPR does not apply since health data are not considered "personal data" as a result,

- If Health Data are considered "personal data" under the GDPR, there may be grounds to assume that Shikari is not liable for any violations of the duties outlined in **Art. 5(1)(f) GDPR**, including the following:

(a) Because processing of Health Data (i.e., collection, analysis, and storage) aims at promoting Ludens' business (i.e., sale of datasets containing anonymized health data to Ludens' clients such as hospitals and research bodies), Ludens is likely to qualify as the "data controller."

(b) Given the, Shikari is (1) unlikely to be eligible as a data controller and (2) might only be eligible as a data processor. In this instance, Shikari was limited to processing Health Data in accordance with Ludens's guidelines (**Art. 28 GDPR**). The security precautions the data processor must take are often specified in these guidelines. Therefore, if there was a breach in the security measures, Ludens, in its function as the data controller, may be held accountable. In any case,

(c) If Shikari is found to have violated the GDPR, it is the patient's responsibility to show that the improper processing caused them to suffer harm. As a result, Ludens, as the data processor, could only be able to support its damage claim after the conclusion of a data protection authority inquiry and a legal battle with the data subjects.

C: Future steps: The following steps should be taken to strengthen Shikari's defense plan:

- To evaluate the data processing contract created by Ludens and Shikari in accordance with **GDPR Article 28**,

- Shikari will give any Health Data information that is accessible, and our company will determine whether Health Data are considered "***personal data.***"